



MASTER OF ADVANCED STUDIES (MAS) IN BUSINESS-LAW- MBL

PRISCA CLAUDIA RENELLA

ELECTRONICAL PRESERVATION OF DOCUMENTS UNDER SWISS LAW

PROF. HENRY PETER

JULY 2007



UNIVERSITÉ
DE GENÈVE

Unil
UNIL | Université de Lausanne

Table of Contents

1	Introduction	2
2	Basic legal obligation according to the Swiss Code of Obligations	2
2.1	Legal obligation to keep book of accounts (Article 957 CO)	3
2.2	Which documents to keep	4
2.2.1	The books	4
2.2.2	Accounting records	6
2.2.3	Special requirements for the balance sheet and the profit and loss statement .	6
2.2.4	Business correspondence	6
2.3	Persons responsible for the preservation.....	12
2.4	Preservation period	13
2.5	Obligation of edition	16
2.6	Forms of preservation	17
2.6.1	Distinguishable Original and copy form.....	18
2.6.2	Undistinguishable original and copy.....	20
3	The archiving process and the archive	22
3.1	General principles of preservation	22
3.1.1	Principles and proper bookkeeping and preservation of books	22
3.1.2	Integrity	23
3.1.3	Documentation	23
3.2	Principles of proper bookkeeping	24
3.2.1	Duty of diligence.....	24
3.2.2	Availability.....	26
3.2.3	Organization.....	26
3.2.4	Archive, access and entry.....	27
4	Consequences of non-compliant behaviour	31
5	Information Carriers	33
5.1	Permissible information carriers	33
5.1.1	Unchangeable information carriers	33
5.1.2	Changeable information carriers	34
5.2	The four conditions of acceptance of the changeable information carriers	34
5.2.1	Integrity of the recorded information.....	35
5.2.2	Time of record.....	40
5.2.3	Compliance with the provisions regarding the use of technical processes at the time of storage and documentation of the processes and procedure for the use of information carriers	42
5.3	Data migration and examination	42
6	Special cases.....	44
6.1	VAT	44
6.2	Income Tax	48
6.3	Recognition of Debt	49
6.4	Dismissal of objection.....	50
6.5	Audit Supervision Act and Article 730c CO	51
6.6	Personal records	52
7	Conclusion.....	53

1 Introduction

Although many companies already have document retention policies in place, they encounter difficulties in being compliant to the different Swiss laws regarding the preservation of documents due to the increasing utilization of technological means for business transactions and correspondence. Technology which will expand even further in future in the area of e-billing, e-tax, e-health among others. Failure to produce all relevant documents in an audit or court proceeding can jeopardize relations to investors, bank customers and lead to disastrous consequences, including fines and imprisonment, as seen in the Enron and WorldCom Cases.

There are two main aspects concerning the preservation of documents: organization and security. It is essential to organize the documents in order to find and access them at any time. Furthermore, the data have to be secured against all risks connected to changes in technology that could, for example, impede any access.

To begin with, this paper shall analyze the legal obligation to preserve documents (Para 2), then it shall explain the process of archiving and the archive (Para 3) and which consequences may arise from non-compliant behavior (Para 4). Finally, this work will set forth the importance of data carriers (Para 5) and illustrate some special cases (Para 6).

Particular attention is dedicated to the aspect of business correspondence, which creates the most difficulties regarding its definition and management in practice. Data protection aspects shall not be discussed as they are not within the scope of this paper.

2 Basic legal obligation according to the Swiss Code of Obligations

The obligation to preserve documents – an important topic that companies must take into account in their organization and management – is provided by several Swiss laws. However, the basis of this obligation is set by the Swiss Code of Obligations (CO) and especially by the regulations regarding commercial accounting (Article 957 et seq.). These regulations provide several basic obligations for companies that are required by the

law to be registered in the Commercial Register¹. The general obligation is to keep books of accounts (§2.1). Para 2.2 of this paper will expose which documents must be kept by a company and Para 2.3 will describe who is responsible for the preservation of those documents. Thereafter, this paper shall illustrate why it is fundamental for the company to be aware of the preservation period (§2.4), the edition obligation (§2.5) and the preservation forms of the mentioned documents (§2.6).

2.1 Legal obligation to keep book of accounts (Article 957 CO)

In 1999, the regulations with regard to commercial accounting in the CO (Article 957 et seq.) were revised. On June 1st 2002, the amended legal regulations took effect, together with the corresponding decree on implementation, the Business Records Ordinance (BRO). The amended rules explicitly provide for the possibility of keeping documents in purely electronic form. As a matter of fact, according to Article 957 Section 2 CO, the books, the accounting records and the business correspondence may be kept and retained in written form, *electronically*, or in similar fashion insofar as conformity with the underlying business transactions remains guaranteed.

Who is obligated to keep and retain such a book of accounts? Article 957 Section 1 CO stipulates that any person or legal entity that is obligated to have his or its company name entered in the Commercial Register must properly keep and retain such books of account as are necessary, to properly reflect the financial situation of the business and to determine liabilities and claims in connection herewith, as well as the operating results of each business year, in accordance with the nature and extent of the business.

Article 934 Section 1 CO and its corresponding Article 52 to 56 of the Ordinance on the Commercial register regulate that anyone² conducting a trading, manufacturing or other business in a commercial manner is obligated to have it entered in the Commercial Register at the domicile of the head office.

¹ Article 934 CO and Articles 52 et seq. Commercial Register Ordinance.

² FORSTMOSER PETER / SPADIN MARCO, *Entwicklungen im Gesellschaftsrecht (Handelgesellschaften und Genossenschaften) und im Wertpapierrecht*, (Erweiterte Fassung des in SJZ 101 [2005] Nr. 21 499 ff. publizierten Beitrages), 2006;
http://rwiweb.uzh.ch/forstmoser/publikationen/pdfdok/Entwicklungen_051025_Internetversion_clean.pdf

Articles 957 to 963 CO do not give a definition of “to properly keep and retain” (see Para 2.2.1 below).

2.2 Which documents to keep

As shown above, the following documents must be kept and retained:

- a) the books,
- b) the accounting records and
- c) the business correspondence.

The balance sheet and the profit and loss statement must be distinguished from the other business books, due to a special requirement of preservation form (see Para 2.2.3).

2.2.1 The books

The law does not explicitly define these terms. However, Article 1 BRO gives a precise indication of what is necessary for proper bookkeeping. This provision stipulates that whoever has a legal obligation to keep records must keep a general ledger as well as sub-ledgers – depending on the type and scope of the company. The general ledger includes:

- a) the accounts (logical structure), on which basis the profit and loss statement and the balance sheet are prepared, and
- b) the journal (chronological structure).

In addition to the general ledger the sub-ledgers must contain all information necessary to assess the financial situation of the company and the obligations and claims relating to the company as well as the operating result of each business year. In particular, it comprises the payroll accounting, the accounts receivable and accounts payable as well as the continuous keeping of the inventories and the unbilled services, respectively (Article 1 Section 3 BRO).

The proper financial accounting (in written form, electronically, or in similar fashion) prescribed in Article 662a CO, must meet the following principals³:

- Exhaustive: any fact which has to be preserved, any income calculation event and any assets establishment must be recorded.
- True: any fact, which has to be preserved, any account event and evaluation must be recorded appropriately.
- Clear: comprehensible for an expert.
- Current: updated regularly.
- Systematically kept: organizing principles as chronology, accounts structure and accounting rules must be observed.
- Appropriate organized: appropriate internal controls must be established.
- Checkable: from the acquisition of data to the business book and profit and loss account.

Any bookkeeping must reflect the above-mentioned principals, regardless of whether there is an obligation to keep the books or not. This means that whoever does keep and retain books of account – even if he is not obligated to do so (e.g. because it's business has a turnover below CHF 100'000 per year) – must observe these principals⁴. In addition several guidelines are available such as the guideline of the Federal Administration⁵, the Swiss Audit Manual⁶ or the recommendations of the Information Systems Audit and Control Association (ISACA Switzerland Chapter)⁷.

³ KOSTKIEWICZ / BERTSCHINGER / BREITSHMID / SCHWANDER, Handbuch zum OR, Zürich, 2002; Schweizer Handbuch der Wirtschaftsprüfung, Treuhand-Kammer, Zürich, 2002; BOSSARD ERNST, in: Zürcher Kommentar, *Die kaufmännische Buchführung*, Artikel 957-964 OR, Teilband V/6/3b, page 124 et seq.

⁴ BOSSARD, page 115 et seq.

⁵ <http://www.kmu.admin.ch/themen/00431/index.html?lang=fr>

⁶ Manuel Suisse d'Audit de la Chambre fiduciaire.

⁷ <http://www.isaca.org/>

2.2.2 Accounting records

Article 962 CO stipulates that the accounting records must be retained. The accounting records include all documents in connection with each entry in the business books that constitute the material proof of the correctness of the accounting⁸. In a proper accounting there is no accounting entry without an accounting record. The definition of accounting records does not create a particular problem. However, the records are absolutely essential for providing evidence of complete and correct financial accounting.

2.2.3 Special requirements for the balance sheet and the profit and loss statement

The balance sheet as well as the profit and loss statement are the documents that have to be established at the end of each business year⁹. They illustrate a summary of all the other accounting documents of the company. These two well known and fundamental accounting documents do not constitute a main problem: Doctrine provides a very detailed definition of the balance sheet and the profit and loss statement¹⁰.

As mentioned before, Article 957 Section 2 CO provides that the books, accounting records, and business correspondence may be kept and retained in written form, electronically, or in similar fashion. Nevertheless, Article 957 Section 3 CO does require the original of the profit and loss statement as well as the balance sheet to be retained in written and signed form.

2.2.4 Business correspondence/ Private correspondence

a) Business correspondence

Article 962 CO also provides for retention of business correspondence. According to the Berner Commentary and the Basler Commentary of Article 962 CO, business correspondence includes all documents exchanged with third parties that provide information of the developments and settlements, which may serve as evidence for

⁸ CALMES JEAN-CHRISTOPHE, Question de droit, in : La question du jour de l'OAV, *De l'archivage électronique*, juillet-août 1999 ; www.oav.ch/Question/07_08_99.html; BOSSARD, page 536 et seq.

⁹ CALMES.

¹⁰ KÄFER KARL, in: Berner Kommentar, *Die kaufmännische Buchführung*, Artikel 957 OR, page 22 et seq.; BOSSARD, page 295 et seq. and page 273 et seq.

business transactions¹¹. BELINGER, LEHMANN, NEUENSCHWANDER and WILDHABER add that business correspondence should cover all significant documents regarding the type and scope of the company¹². The question that immediately arises is: What is a significant document? One cannot be certain at the moment of archiving that a document will not be of significance in the future. What is required in a future's legal proceeding often will only become apparent at a later stage. Theoretically, any document can become of importance in a legal proceeding. A meeting invitation per e-mail, for example, may at first glance be a worthless document. This document can still become significant if one has to prove that a certain person took notice of a particular issue that was to be discussed at that precise meeting. The proof of this person's knowledge of the issue is often a capital aspect, e.g. in penal law¹³. If the invitation e-mail was not duly preserved, making it impossible to prove that this person actually acknowledged the mentioned issue, this person could evade a conviction.

Therefore, such a retrospective definition is not helpful. A company must be able to define in advance which documents must be available for evidence in the future. The company, in my opinion, can select with the help of a business risk approach, in which areas the risk of loss of evidence can be taken and for which areas all evidences have to be kept and retained. This business risk approach is possible only with regard to business correspondence. Any document, which is either book or accounting record, has to be imperatively preserved (See Para 2.2.1 and 2.2.2 above).

Thus, this business risk approach allows the company to define the categories or functions of employees who have to preserve their business correspondence documents for ten years and the ones which are not obliged to retain any business documentation.

For example, a company may decide that the employees involved in the assembly line work do not have to preserve their documents, contrary to those responsible for placing orders. A manufacturer of MP3 players may take the business risk to preserve documents

¹¹ SCHNURRENBERGER CATHRIN, *Datenaufbewahrungspflicht – ein Minenfeld für den VR*; <http://www.itandlaw.ch/html/set/publikationen.html>; NEUHAUS MARKUS / BINZ PETER, in: *Kommentar zum Schweizerischen Privatrecht, Obligationsrecht II*, Basel/Frankfurt a.M., 2002, Art. 962 N 7.

¹² BELINGER JACQUES / LEHMANN BEAT / NEUENSCHWANDER PETER / WILDHABER BRUNO, *Records management, Leitfaden zur Compliance bei Aufbewahrung von elektronischen Dokumenten in Wirtschaft und Verwaltung mit Checklisten, Mustern und Vorlagen*, 2004, page 151.

¹³ Article 144bis Section 2 Swiss Penal Code regarding data deterioration; Article 305bis Swiss Penal Code regarding money laundering.

relating to the quality check of its players produced only for a period little longer than the warranty period¹⁴, because the risk of being sued after expiration of the warranty period is minimal. In these cases, the preservation period of ten years cannot be properly justified.

The situation is different for a manufacturer of barbecue grills for example, who seriously risks falling under the Federal Act relating on Product Liability. Contrarily, the risk that someone may be killed or injured by an MP3 player or that the latter damages an object of private use is extremely minimal¹⁵. The barbecue grill producer faces a far bigger chance of being sued. The Federal Act relating on Product Liability provides a statute of limitation of ten years in Article 10, therefore the barbecue grill producer should retain its business correspondence documents for slightly longer than ten years. Hence, each company is free to define the business risk they want to take.

All the definitions of business correspondence found in the doctrine are flexible and take technological evolution into consideration. The Berner and Basler Commentary and several authors provide examples of business correspondence in form of a non-exhaustive list¹⁶. Thus, we can conclude that private correspondence and advertisements basically do not fall under the definition of business correspondence.

The awareness of employees that they must gather and systematically archive correspondence in the form of physical letters is generally quite high. Processes are often established within companies and defined in a set of instructions (“Filing Policy”)¹⁷. The situation is different as far as electronic correspondence is concerned. With a few exceptions, Swiss companies only keep archives in paper form. This means that all relevant e-mails would have to be printed out and systematically added to the paper files. This can create space problems and lead to inefficient work flows.

¹⁴ It could be possible to be sued just before expiration of the warranty. In this case, because it takes a certain time to serve a writ, 2-3 months would be appropriate as additional preservation period.

¹⁵ Article 1 Federal Act relating on Product Liability.

¹⁶ Incoming and outgoing letters, contracts, telegrams, facsimiles, e-mails, internal notes, contracts, bills, delivery notes or receipts, invoices and banking documents, articles of incorporation, charters, records of cases, corporate legacy documents, judicial decisions and documents regarding public authorities and contracts for work labour are considered to be business correspondence. See CALMES.

¹⁷ ERNST & YOUNG, in : Legal News, *L'ordonnance concernant la tenue et la conservation des livres de comptes en pratique*, January 2006 ;
http://www.comptaval.ch/backoffice/images/newsfichiers/newsFichier_142.pdf.

b) Private correspondence

Employees often believe that their mailboxes, together with the e-mail archive, are regularly backed up and then archived in compliance with the law. But that is often not the case. E-mail archives are very often only backed up purely for disaster recovery purposes. Such a back-up method is significantly different from a systematic archiving process. Important documents that must be retained by law could get lost if not systematically archived.

In addition, with the technological evolution and especially today's widespread use of e-mails¹⁸ and mobile texts, for example, not only in business, but also in private correspondence, private and business correspondence end up in the same mailbox. Moreover, as a matter of fact, it is not unusual to send an e-mail containing both elements (private and business). All the documents exchanged with third parties that are clearly of a business nature, such as formal letters, contracts, bills, delivery notes or receipts, invoices and banking documents, do not create a particular problem. These documents have to be preserved.

There are no problems with emails, mobile texts and internal notes, as long as employees systematically distinguish and classify them based on the content of the correspondence. However, close business relations often coincide with the exchange of personal matters and therefore also business related mails may have private elements. At this point, data protection aspects (which are not within the scope of this work) should be kept in mind.

The Federal law on Data Protection (FDP) provides that the privacy and fundamental rights of persons about whom data are processed may be protected. Therefore, a third party should ask prior consent from the concerned person for reading an e-mail including private elements. If the company explicitly prohibits private use of e-mails in the company, any third party can read the e-mails at any time without prior consent of the concerned person, even if it contains private elements. In such cases, the concerned employee should know that it is prohibited to use the company's e-mail system for private use and thus accepts that his private e-mails may be read by a third party. In my opinion it should be always possible to access and read e-mails sent from the company's e-mail

¹⁸ SCHELLENBERG WITTMER AVOCATS, in : Newsletter, *Les données électroniques dans le monde des affaires: une nouvelle loi et des développements récents*, April 2005; http://www.swlegal.ch/downloads/newsletters/SWnews_0405F.pdf.

system without prior consent from the concerned person, because anyone knows that e-mails can be forwarded and modified in a very easy manner. Each time an employee sends a private e-mail he or she takes the risk that someone other than the receiver reads it without his or her prior consent. Thus, when writing private elements in a company e-mail, the employee, in my opinion, accepts that a third party could read his or her private e-mails. Furthermore, one should note that it is always possible to send e-mails with a private e-mail account. In doing so, the employee clearly states that the e-mail is private and thus protected by data protection law.

In order to avoid such unclear situations, the company has to inform its employees and establish clear rules about the use of this kind of correspondence¹⁹:

- The use of e-mails in the business process should be clearly regulated and documented.
- Electronic business transactions should be set forth in a clear E-Business Agreement²⁰.
- For each relevant business transaction a confirmation (return receipt) should be requested which can be retraced in the system afterwards.
- The preservation of the complete electronic communication.
- Set clear rules concerning the use of e-mails in the company (for example, prohibition of private use or acceptance of rules in connection with the preservation and deletion of emails).
- Emails should be classified by and per user.
- The general recording of e-mails is a special case of archiving and accordingly the filing of business correspondence (“day copies”). The recording can be facilitated with

¹⁹ BELINGER / LEHMANN / NEUENSCHWANDER / WILDHABER, page 120 et seq.

²⁰ Such as *Electronic Data Interchange (EDI)* and *EDI for Administration, Commerce and Transport*. EDI is a set of standards for structuring information to be electronically exchanged between and within businesses, organizations, government entities and other groups. The standards describe structures that emulate documents, for example purchase orders to automate purchasing. The term EDI is also used to refer to the implementation and operation of systems and processes for creating, transmitting, and receiving EDI documents. EDIFACT is the international EDI standard developed under the United Nations.

the above-mentioned points. E-mail recording without any classification should be absolutely avoided. This is possible with clear handling of corporate management and consistent application of the implementation principles.

As illustrated above, in the future e-mails are likely to be considered more and more as a data source in legal procedures²¹. Authorities may also request the issuance of documents in case the information sought by them does not or not directly concern the business. The selection of the documents that must be preserved may turn out to be a major organizational burden. However, the risk of not being able to fulfill requests of document issuance may be estimated to be much severer.

“In addition, information technology that has enabled companies to operate more efficiently has now become an issue of efficiently capturing, managing, storing, preserving and delivering contents and documents such as e-mails (...)”²². Therefore, the problem is not only the nature of the business correspondence but also its management. “Companies’ major challenge is dealing with unstructured and fixed data, which are comprised of textual objects such as office documents, e-mails, and e-mail attachments amongst others as well as image, video or audio files”²³. Thus, if the Company establishes clear rules and educates its employees regarding the management of these documents, the problem may be slightly reduced.

“Many organizations have also enacted mailbox quota, which force e-mail users to archive or delete their e-mails and attachments without their control as soon as the mailbox exceeds a certain size. Unfortunately, employees spend a large amount of their time at work browsing archived mailboxes and file systems for the required e-mails, attachments and documents. Hence the digital archive appears to have become the preferred alternative”²⁴.

c) Revision of company and accounting legislation

A revision of company and accounting legislation is already planned. Swiss company law is to be comprehensively modernized and brought in line with the needs of the economy.

²¹ SCHELLENBERG WITTMER AVOCATS.

²² BLIGGENSTORFER SIMON, *Records Management*, Individual Assignment Paper CIB_01/06, Private Hochschule für Wirtschaft, 12 February 2007, page 4.

²³ BLIGGENSTORFER, page 4.

²⁴ BLIGGENSTORFER, page 7.

Corporate governance, in particular, is to be improved, new rules on capital structures and accounting and reporting requirements will be introduced, and the provisions governing annual general meetings will be updated. On December 2nd, 2005, the Federal Council opened committee hearings on the revision of company and accounting legislation, and on February 14th, 2007, it collected the results of the consultation and gave the Federal Department of Justice and Police the task of formulating an Opinion. A preliminary draft of the revised legislation has already been written; this draft has deleted business correspondence as documents to be preserved.

Does the fact that the preliminary draft does not name the business correspondence as documents needing to be preserved change anything? As mentioned above, business correspondence is essential regarding evidence in case of any disputes. In my opinion, the companies, if they want to be on the safe side, should not change their organization and management regarding business correspondence. The only difference between the preliminary draft and the actual law is that the company, from a civil law perspective, will not be obliged to preserve the business correspondence and therefore cannot be ordered to produce it in front of a court (Article 963 CO). In addition to that, from a penal law perspective, whoever fails to preserve only the business correspondence does not fulfill the conditions stipulated in Article 166 Swiss Penal Code (SPC) regarding failure to keep books and Article 325 SPC regarding irregular keeping of books (see Para 4) and will hence not be incriminated.

2.3 Persons responsible for the preservation

Article 961 CO sets forth the responsible persons for the preservation in the different types of companies / legal entities. First of all the profit and loss statement and the balance sheet must be signed by the company owner or, if applicable, by all of the personally liable partners. If the legal entity is a corporation, a corporation with unlimited partners, a limited liability company or a cooperative, these documents must be signed by the persons entrusted with the management. The signature constitutes the primary obligation of accounting²⁵. The responsible persons must therefore also preserve all the relevant documents necessary for the accounting.

²⁵ BOSSARD, page 295 et seq. and page 169 and 519 et seq.

This disposition is fundamental in case of non-compliant preservation of the documents. As a matter of fact, the consequences of a failure to keep books or an irregular keeping of books can have severe consequences for the responsible person (See Para 4 below). In my opinion, the final step in the pyramid of responsibilities for the preservation of documents is the board of directors. The latter is entrusted with the management and must decide about the issue of preservation. The board of directors, which represents the company (Article 55 Swiss Civil Code, CC), is therefore responsible if, due to the deficient organization of the enterprise, a failure to keep books or an irregular keeping of books cannot be attributed to a natural person (Article 102 SPC, see Para 4 below). However, in my opinion it is unlikely that such failure cannot be attributed to a natural person. The responsibility must be established case by case, but from my point of view, the company itself has a smaller risk of being punished than the employee.

2.4 Preservation period

According to Article 962 CO, the business books, accounting records and business correspondence must be retained for a period of ten years. The retention period shall begin with the expiration of the business year in which the last entries were made, the accounting records were established and the business correspondence was received or sent. The start of this period is the end of the business year and not the end of the calendar year²⁶. This period has a practical aspect in being the same as the one provided by Article 127 CO (ordinary prescription).

Swiss law sets forth a preservation period of ten years for the business books, accounting records and business correspondence (which include, as seen above, most documents except private correspondence and advertisement), though some documents should, in my opinion, be preserved for a longer period of time.

The table below shows the *suggested* preservation period and the start of this period for documents, which are, according my point of view, fundamental in the existence of a company. However, this table is an example; each company is free to define which preservation period it will apply since the period provided by Article 962 CO is fulfilled.

²⁶ BELINGER / LEHMANN / NEUENSCHWANDER / WILDHABER, page 37.

Documents	Suggested preservation period	Start of the preservation period
<ul style="list-style-type: none"> • Articles of association • Excerpt from the commercial register • Register of shareholders • Minutes of General shareholder meetings • Administrative acts (minutes, audit reports, etc.) • Agreement of share purchase and sale contracts 	Period of existence of the company	Establishment of the document
Insurance policies	Policy period + 10 years	Establishment of the policy (at the end of the policy, the preservation period of ten year will start)
Documents concerning the employees	Employee's contract period + 10 years*	Establishment of the contract / establishment of the document
Documents regarding the buildings (Mortgage, leasing agreement, receipt for lease security deposit, etc.)	Occupation period + 10 years	Establishment of the document

<ul style="list-style-type: none"> • Credits • Billings • Securities, stocks and bonds 	11 years	Upon expiration of the business year in which the last entry in the business book has been made
Bank guarantees and other leasing contracts	Guarantee / leasing period + 10 years	Establishment of the guarantee / leasing
Intellectual property documents	<ul style="list-style-type: none"> • Patents: 20 years • Trademarks: unlimited period • Designs: 25 years • Copyright: 70 years (50 years for software) 	<p style="text-align: center;">Date of filing</p> <p style="text-align: center;">(Copyright : after the death of the author)</p>
Company guidelines, instructions	Period of existence of the guideline / instructions	Establishment of the guideline / instructions

* For ratings documents, reference letters, employment applications, etc. the period of preservation may be shorter if considered to be business correspondence, see Para 2.2.4 above and Para 6.6 below.

As shown in the table above the preservation period depends on the type of document. As mentioned above, Companies are free to define the preservation period for such documents that are considered to be business correspondence (see Para 2.2.4). In my opinion, companies should, as a general rule, add one year to the legal or chosen preservation period. The reason of this additional year is the following: As mentioned before, the retention period begins with the expiration of the business year in which the last entries were made, the accounting records were established and the business correspondence was received or sent. In practice the deletion of documents is usually

programmed depending on the storage or the last amendment date. The ten year period may be too short, because if the start of this period is the expiration of the business year and not the storage or the last amendment date, some documents may already be deleted before the end of the legal period. Adding one additional year is opportune for avoiding the deletion of documents that do not yet fulfill the ten year preservation period.

Several authors²⁷ recommend longer preservation periods. Unfortunately they do not state their reason for recommending the additional years.

In principle, because nowadays technology enables the storage of large amounts of information, it is always better to preserve documents which are deemed to be relevant for the company business²⁸. As a matter of fact, if the company lacks evidence, its position in the case of a legal dispute may be weakened considerably. The consequences of lack of evidence can be very costly.

2.5 Obligation of edition

Art. 963 CO stipulates that whoever is obliged to keep business books may, in the case of disputes regarding the business, be ordered to produce the business books, accounting records and business correspondence, if an interest worthy of being protected is brought forth and if the court deems it necessary for evidence purposes. Additionally, if the business books, accounting records or business correspondence are retained in electronic or similar form, the court or the authority that has the competence to request the production by virtue of public law may also order that:

- 1) The documentation be produced in a form that is readable without auxiliary means, or
- 2) The means to make the documentation readable be provided.

²⁷ BELINGER / LEHMANN / NEUENSCHWANDER / WILDHABER, page 175 et seq.; HAYWARD DENISE, in: Archives et législation, 2005.

²⁸ Discussion with Prof. Dr. Ing. Karl-Heinz Rödiger, Fachbereich Mathematik/Informatik, Bremen University, during the Seminar „15 Jahre Internetnutzung - Stand und Perspektiven“ of the Europa Institut an der Universität Zürich, 21 June 2007.

The purpose of this provision is to avoid overflowing the court with papers, which is a well-known strategy in certain foreign cases, making it difficult to examine the documents and possibly delaying the procedure²⁹.

This is the minimal regulation which the Swiss Code of Obligations sets forth for the edition obligation. If the procedure does not concern a commercial accounting responsible, a conflict regarding his business or the edition of business books, accounting records and business correspondence, cantonal procedure law might stipulate further rules of edition³⁰.

2.6 Forms of preservation

As mentioned above, the law stipulates that the books, accounting records and business correspondence must be kept and retained in written form, electronically, or in similar fashion. By including “or in similar fashion”, Article 957 Section 2 CO takes technological evolution into consideration, and “theoretically” these forms have the same force of evidence (Article 957 Section 4 CO). It should therefore be possible to preserve all the documents, except the balance sheet and the profit and loss statement (see above Para 2.2.3, Article 957 Section 3 CO), exclusively in electronic form. I wrote “theoretically”, because in practice there is, in some cases (see Para 2.6.1 below), a difference concerning the force of evidence between a document commonly considered to be “original” and a “copy” document³¹. According to the Message regarding the revision of the heading thirty-two of the Swiss Code of Obligations³², a document such as the balance sheet and the profit and loss statement which have to be retained in written and signed form, is considered to be an “original” document. A validly signed photocopy or validly signed duplication may also be considered an original³³. GASSER/HÄUSERMANN³⁴

²⁹ Message concernant la révision du Titre trente-deuxième du code des obligations (de la comptabilité commerciale) du 31 mars 1999 ; <http://www.admin.ch/ch/f/ff/1999/4753.pdf>.

³⁰ KÄFER, page 1179.

³¹ For example scanning of a paper-based document.

³² Message concernant la révision du Titre trente-deuxième du code des obligations (de la comptabilité commerciale) du 31 mars 1999.

³³ BELINGER / LEHMANN / NEUENSCHWANDER / WILDHABER, page 33.

³⁴ URS GASSER/ DANIEL MARKUS HÄUSERMANN, in : *Beweisrechtlich Hindernisse bei der Digitalisierung von Unternehmensinformationen*, AJP/PJA 3/2006.

add the issue where “original” and “copy” are not distinguishable³⁵ (See Para 2.6.2 below).

First, we shall analyze the issue, where the original and copy form can be distinguished and then we shall analyze the issue, where these two forms are not distinguishable³⁶.

2.6.1 Distinguishable Original and copy form

In the seventies, paper was the only carrier of correspondence and accounting documentation³⁷. The information of the physical carrier which was readable without the help of other instruments was considered original. Afterwards, this information was transferred and recorded on modern information carriers, data carriers or image carriers. This guaranteed faster access, better organization and a gain of space. Nowadays the electronic business correspondence has its source on data carriers, accounting is established electronically and business books are kept electronically. As mentioned above, according to Article 957 Section 4 CO these forms “theoretically” have the same force of evidence. However, in practice there is still a difference regarding the force of evidence.

Companies are perfectly in compliance with the law if they preserve their documents exclusively in electronic form, but they do take a risk from a civil law point of view. As a matter of fact electronic records of paper-based documents are equal to photocopies, and the probative force of the latter is contested in doctrine. BÜHLER³⁸ states that photocopies have the same probative force as an original document in the majority of the procedural laws. SCHLAURI³⁹, on the contrary, states that the photocopies have extremely weak probative force, similar to unsigned documents. The practice of the courts differentiates between an electronic record and an original document, especially with regard to the question of authenticity of the evidence. This issue is not treated by Article 975 Section 4 CO nor by the UNCITRAL Model Law on Electronic Commerce Guide, that provides

³⁵ E.g. “*genuin elektronischen Dokumente*”, i.e. documents that are established and exclusively retained in electronic form; no paper-based form of this document exists.

³⁶ FF 1999 5152; <http://www.admin.ch/ch/f/ff/index.html>.

³⁷ Message concernant la révision du Titre trente-deuxième du code des obligations (de la comptabilité commerciale) du 31 mars 1999.

³⁸ BÜHLER ALFRED, „Die Beweiswürdigung“, in: Christoph Leuenberger (Hrsg.), *Der Beweis im Zivilprozess*, Bern 2000, 71 ff., 80.

³⁹ SCHLAURI SIMON, *Elektronische Signatures*, Zürich 2002, Rz. 655.

that, where the law requires information to be presented or retained in its original form, the requirement is met by a data message if:

- a) There exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
- b) Where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented⁴⁰.

If the authenticity of a signature on an electronic recorded document for example is contested, the party that has the burden of proof must prove the authenticity of the signature, comparable to a photocopy. A graphology expertise is required and the burdened party must present the uncontested signature to the expert in original form. If all the original documents with this signature were destroyed after their scanning, the party carrying the burden of proof risks to fail in proving authenticity of the evidence. Therefore, as a rule, I recommend preserving all the originally signed documents in paper-based form, such as the balance sheet and the profit and loss statement, or at least preserving one example of original signature in order to avoid failure of proof of the document's authenticity.

It might be different for handwritten notes made during a discussion with clients, for example. In this case the probability that an electronic record of it will be accepted as proof of authenticity is much higher.

The electronic preservation form includes the data carrier and the image carrier. A "data carrier" is any type of medium that is capable of holding data, such as a hard disk drive. An "image carrier" can be film, plates, cylinder, screens, or other transfer mediums that hold an image for reproduction.

Business books, inventory, vouchers and business correspondence can be preserved either in written and signed form, or with image or data carrier, as shown in the table below.

⁴⁰ UNCITRAL Model Law on Electronic Commerce Guide to Enactment with 1996 with additional article 5 as adopted in 1998bis.

2.6.2 Undistinguishable original and copy

The FF 1999 5162 provide that in practice the books, accounting records, and business correspondence are generally established and exclusively retained in electronic form; no paper-based form of these document exists⁴¹. GASSER/HÄUSERMANN speak of *genuinely electronic documents*, which, according to the FF 1999 5164, should be treated as originals. Indeed, the printed form of these documents is in fact the copy of it.

If no relevant information is lost during the treatment (scanning or printing for example), original and copy are considered to be undistinguishable. From a civil law perspective these documents have absolutely the same force of evidence.

This category basically includes two types of documents: documents that have already been copied in their final form and documents with no added handwritten notes. The first type of document is typically the one exclusively established in electronic form, printed and stored afterwards without any added notes or remarks. As an example: a photocopy of a contract draft or a bank account statement is in fact the “copy” (printed copy) of the electronic version. Also documents that are only available as photocopies such as outbound correspondence fall into this category of document type. The second type of document does not include handwritten additions, such as a date or receipt stamp. In principle, no relevant information is lost in reproducing this document by photocopy or scan. The exception to the rule regarding this last type of document: is when a company uses stamps of identical type, but of different colours, and the copy of the document is only black/white. However, in any case these documents usually also include a signature and therefore fall into the category where original and copy are distinguishable (Para 2.6.1 above)⁴².

⁴¹ See also FF 1999 5163 and FF 1999 5152.

⁴² GASSER/HÄUSERMANN.

The following table shows which documents have to be kept in which form:

Document	In written form	Electronically		Similar form
		Image carrier	Data carrier	
Balance sheet and loss and profit statement	X (and signed according to Article 957 Section 3 CO)			
Business books and inventory	X	X	X	X
Vouchers and business correspondence	X	X	X	X

3 The archiving process and the archive

The Business Record Ordinance distinguishes the general principles of preservation regarding the principles of proper bookkeeping (in general) and preservation of book (Article 2 BRO), integrity (Article 3 BRO), and documentation (Article 4 BRO), from the principles of proper bookkeeping regarding the duty of diligence (Article 5 BRO), availability (Article 6 BRO), organization (Article 7 BRO), and archive, access and entry (Article 8 BRO).

3.1 General principles of preservation

The general principles of preservation take the “proper bookkeeping” concept up of Article 957 Section 1 CO. Several accepted guidelines may help companies to fulfill their obligation of proper bookkeeping regarding the preservation of the books (Para 3.1.1). In addition, companies shall ensure the integrity of their books, vouchers and business correspondence (Para 3.1.2) and document the instructions in order to understand these books, vouchers and business correspondence (Para 3.1.3).

3.1.1 Principles and proper bookkeeping and preservation of books

According to the Article 2 Section 1 BRO the Generally Accepted Accounting Principles (GAAP) in business must be observed (proper bookkeeping) when keeping the books and recording the vouchers. The meaning of “to properly keep and retain” has already been discussed in the above Para 2.2.1 of this paper. However, Article 2 Section 2 BRO provides that if the books are kept and preserved electronically or in similar manner and if the accounting records and the business correspondence are recorded and kept electronically or in a similar manner, the generally accepted principles of proper data processing must be observed as well. In case the Ordinance or any decrees based on it do not contain any provisions, proper data processing is determined by generally accepted compilations of rules and recommendations of expert bodies (Article 2 Section 3 BRO). Many generally accepted guidelines and bodies of rules and regulations, such as the COBIT directive (Control Objectives for Information and related Technology of the Information Systems Audit and Control Association ISACA), help many organizations fulfill the conditions of “proper data processing”. COBIT is an IT governance framework

and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. ITGI's latest version - COBIT 4.0 – enables alignment and simplifies implementation of the COBIT framework. COBIT presents activities in a more streamlined and practical manner, so that continuous improvement in IT governance is easier than ever to achieve⁴³. COBIT has become the integrator for IT best practice and the umbrella for IT governance because it is harmonized with other standards and continuously kept up to date. The process structure of COBIT, combined with its high-level business oriented approach, provides an end-to-end view of IT that aids organizations in getting the most value possible from their IT investments.

3.1.2 Integrity

Article 3 BRO stipulates that the books must be kept and preserved and that vouchers and business correspondence must be recorded and retained in such a manner that they cannot be altered without the alternation being recognizable. The integrity and authenticity must be guaranteed, i.e. the business transaction, which is recorded, may correspond to the underlying fact and the use of the latter may be done without error and in an unaltered manner⁴⁴.

This requirement is new and should lead to several modifications of the electronic process of bookkeeping and of electronic preservation⁴⁵. Systematic internal controls and security measures concerning the processes and the preservation, such as e.g. digital signature, access safety and logging, may help fulfill this new requirement of the Business Record Ordinance.

3.1.3 Documentation

Depending on the type and scope of business, organization, competences, processes and procedures as well as infrastructure (machines and programs) that is used in order to keep

⁴³ GOVERNANCE INSTITUTE, COBIT 4.0, *The newest evolution of Control Objective and related Technology, the world's leading IT control and governance framework* (www.itgi.org and www.isaca.org/cobit).

⁴⁴ BELINGER / LEHMANN / NEUENSCHWANDER / WILDHABER, page 39.

⁴⁵ ABAKUS, *Elektronische Archivierung – Gesetzlich Anerkannt*, 2002; www.abacus.ch/downloads/pages/2002-03/s18-23.pdf.

and preserve the books, the instructions must be documented in a manner that the books, vouchers and business correspondence can be understood (Article 4 Section 1 BRO). The instructions shall be updated and be preserved according to the same principles and for the same period of time as the books kept in accordance with such instructions (Article 4 Section 2 BRO).

The principal of this article provides that each business transaction should be recorded in a traceable manner. The business transaction must be clearly and systematically arranged and entered into the underlying voucher account with a reference number so that the expert understands the accounting books, the accounting records and the business correspondence⁴⁶. The verifiability requires that transactions must be retraced in unaltered form and convenience requires that all the organizational, operative and technical measures according to type and scope of business and circumstances which are necessary to establish the financial key data must be respected.

3.2 Principles of proper bookkeeping

Contrary to the general principles of preservation, the following Para regarding the principles of proper bookkeeping provide that the books, the vouchers and the business correspondence are to be preserved carefully, systematically, and shall be protected against harmful effects (Para 3.2.1). In addition, companies shall keep these documents and the equipments and technical means available for inspection and examination (Para 3.2.2). Finally, companies have to take particular care about the organization of the archived documents and the archive itself which are essential topics (Para 3.2.3 and 3.2.4).

3.2.1 Duty of diligence

According to Article 5 BRO the books, the vouchers, and the business correspondence are to be preserved carefully, systematically, and shall be protected against harmful effects.

The choice of archive, access and entry are essential (see Para 3.2.4); the organization is also of significance (see Para 3.2.3).

⁴⁶ ABAKUS ;www.abacus.ch/downloads/pages/2002-03/s18-23.pdf.

In order to preserve the information carefully and protect it efficiently, with the possibility to preserve the documents electronically, new solutions have to be considered for storage, archiving and recovery of the data⁴⁷. Several facilities are at the disposal of companies⁴⁸. However, these facilities are not required by law.

Concerning the storage place of data, three main problems arise from the fact that the documents have to be preserved at least for a decade:

- a) Access to old hardware and software,
- b) Deterioration of electronic carriers and
- c) Storage places that offer a high level of protection.

Concerning the access to old hardware and software, a machine park of all different generations will have to be preserved or transcription software will have to be written at each informatics application's exit (regular data migration; see Para 5.3).

A solution has to be found for the rapid deterioration of electronic carriers. As a matter of fact, if paper has proven its longevity, the disks of the 70ties have been replaced by the floppy of the 80ties and the CD-Rom of the 90ties and the USB stick will certainly also be replaced by the coming technology. Microfilm can be an alternative: The colored photos can store a huge quantity of data ensuring access for several centuries. In addition, its process invented by the Lumière brothers is one of the simplest ones.

The choice of the storage place is essential to protect the documentation to preserve from natural disasters (flood disaster, earth quake, fire, etc.) and access from non-authorized persons. Since the reorganization of the Swiss Army, it has been possible to buy bunkers as storage places. These are sold to companies specialized in archiving and secure storage. The physical protection of these bunkers is very high and can be completed by modern control systems of the new generation, e.g. identification systems inalienably relayed to the authorized person such as iris scans or digital fingerprints. However as mentioned above, it is not necessary to preserve the documents in such bunkers in order

⁴⁷ WUERGLER RAOUL OLIVIER, in : Banque & Finance, *Une chaîne de haute sécurité pour les données sensibles*, Septembre – Octobre 2006.

⁴⁸ It is possible to plan a high level of security and protection system for sensitive information. This is especially the case for banks, but also for other companies. More and more international companies desire to find solutions that efficiently protect their sensitive information.

to be compliant with the law. A simple room in the company building, which ensures the preservation of documents during the entire preservation period, is perfectly sufficient to fulfill the law.

3.2.2 Availability

Article 6 Section 1 BRO stipulates that the books, vouchers and business correspondence should be preserved in such a manner that they can be inspected and examined by an authorized person within an appropriate period of time until the end of the preservation period. If required for inspection and examination, the appropriate personnel as well as the equipment or technical means should be kept available. Within the scope of the right to inspection and upon request of an authorized person there must be a possibility to make the books readable without technical means (Article 6 Section 2 and 3 BRO).

In this context, what is “an appropriate period of time”? A particular document whose illustration, examination, or eventual transfer does exclusively exist electronically, cannot be found in some seconds by the day-to-day business IT-system, but only after hours or days. The reason for this waiting period is the specific requests in an archive system with a huge amount of data, preserved over ten years. The “appropriate period of time” requirement of the Swiss law is fulfilled when the archive system furnishes the requested information within 1-2 weeks. The requested information may be understood and controlled within this period of time⁴⁹.

3.2.3 Organization

According to Article 7 Section 1 and 2 BRO, archived information shall be separated from current information or shall be marked in a way that distinction is possible, respectively. The responsibility for the archived information shall be clearly regulated and documented. Archived information must be accessible within an appropriate period of time.

The information is subject to limited and regulated access requirements and to specific liability of a day-to-day archive body that is independent of the business. The entries to the archived data should be reserved for “authorized persons” such as e.g. identified archivists or auditors, should be subject to logging. Archive systems are not suited for the

⁴⁹ BELINGER / LEHMANN / NEUENSCHWANDER / WILDHABER, page 158.

day-to-day business planning, because of the long-term and secure requirements of preservation of the recorded information. It is possible, and in many cases also recommended, that the information concerning the business records that is destined for the type and scope of business and transferred in the archive, stay available for a certain period of time.

Costly IT recovery systems are not needed, in my opinion, if we take into account the amount of information that companies have to keep and retain. As a matter of fact, each employee organizes and stores his or her documents partly in electronic files and partly in paper-based format. The amount of information to preserve is therefore divided by and per user. As a rule however, I strongly recommend to avoid organizing the documents chronologically or by sender, because in case of a legal dispute, the company will be obliged to produce documents concerning a very precise issue. At that moment, it will be indispensable for the company to be able to distinguish between an e-mail confirming a meeting or a purchase order. The chronological storage is much more inefficient than the storage by sender. Each employee should therefore organize his or her documents by client or mandate.

3.2.4 Archive, access and entry

The information shall be inventoried systematically and shall be protected against unauthorized access. Accesses and entries shall be logged. Such logs are subject to the same obligations of preservation as the data carriers (Article 8 BRO).

The following principals were developed by the practice and constitute a guideline for proper archiving⁵⁰:

- Each document disposes of a clear classing and classification: Miscellaneous documents have to be classed (put into folders per mandate or client) and classified respectively (put these folders in alphabetical order or in order of importance, for example). This procedure of classing and classification depends on the requirements of the company's business.
- Each document disposes of an index/description that is independent of the format: An archive system must be able to record all the different data format. It is necessary to

⁵⁰ BELINGER / LEHMANN / NEUENSCHWANDER / WILDHABER, page 128-129.

install different search means in order to find documents that are preserved for a very long period of time at all times. Traditionally, a separate index or document description respectively have to be appointed under a single format.

- The documents must be archived in an exhaustive and unchangeable manner: The technical integrity is ensured by several measures. The control system can e.g. cover the processing of documents, the input for the registration of the data, checksum and cryptographic mechanism. “Unchangeable” means that a document that has been recorded with a specific format cannot be altered without the alteration being recognizable. This principal does widen the requirements of the control system.
- Each document has to be archived in its last version: the archiving has to be done according the classification. The valid version must be visible from type of classification. The company should avoid preserving different versions of a document concerning the same business transactions or facts if not explicitly required (e.g. by different developing steps of a product).
- A business transaction has to be traceable within an appropriate period of time: The principal of traceability is imperative. The only scope of interpretation concerns the length of the “appropriate” period of time. It could be possible to define this period of time by the amount of use, which makes sense in the active systems. The records means and the storage types are derived from this. However, an absolute long term archiving system does not usually allow access to the data within a specific period of time for the requirements of day-to-day business. As guideline, one week should be the limit for long term archives, in order to be considered as appropriate period of time according to Article 6 BRO.
- The data migration to a new archive system has to be possible without any information loss: See Para 4.4 concerning the data migration.
- All relevant acts in the archive have to be logged: Like all important IT systems, the most important procedures have to be verified and logged. “Verification” means active verification that allows an immediate reaction. It also provides the basis for the rating of the Key Performance Indicators (KPI) and the Key Global Indicators (KGI) under IT Governance Guidelines.

- The archived data can only be deleted through a controlled procedure: The data have to be deleted with a proper verification. The physical destruction of the unchangeable information carriers is the main method. The deletion must also be recorded.

A detailed archiving concept encompassing both electronic and traditional paper-based archiving is a prerequisite for the regulatory compliant archiving of business relevant document. An archiving concept should list per business process what documents need to be archived for what period. Additionally, the archiving concept should include a description of both organizational and technical measures to ensure the archiving of the relevant business documentation. Seamless and complete archiving of all business-relevant documentation is only possible if the archiving process is aligned to and integrated with the existing business processes and if the responsibilities for the archiving are clearly specified. Employees must be adequately trained and awareness of the need to archive business documentation has to be created⁵¹.

As already mentioned above, both, physical and logical access to the archive must be logged. Thus, access to the archived data has to be restricted to authorized persons only, appropriately controlled and monitored, i.e. any physical or logical access has to be detected and logged. This is not only applicable for the archiving application itself, but also for the underlying infrastructure, e.g. databases, servers and archiving media. A periodic review of the access logs and the access control list should be implemented, again including both physical and logical access to the electronic archiving system.

However, the security concept for the electronic archiving system should not only consider access to archived data. Environmental security has to be considered as well, including a comprehensive backup and recovery concept⁵². In addition the electronic archive should be included into the central Patch Management strategy.

Usually business documentation needs to be archived for 10 years or longer (also see Para. 6 concerning special cases). Thus, strategies to ensure the long-term availability to the archived information are essential. This does not only apply for the data itself, but also

⁵¹ ERNST & YOUNG, *Elektronische Archivierung*, 2007.

⁵² ERNST & YOUNG, *Elektronische Archivierung*, 2007.

for the applications and the infrastructure underlying the archiving solution, the archiving media and the knowledge how to access and retrieve archived information⁵³.

As mentioned in Para 2.4 if the company lacks evidence, its position in the case of a legal dispute may be considerably weakened. The consequences of such lack of evidence can be very costly. Furthermore, insufficient recording and archiving of business-related information can increase the risk of incorrect management decisions due to an incomplete management information basis. Additionally, an archiving solution that is not aligned and integrated with a company's existing business process is likely to result in additional redundancies and increased costs⁵⁴.

Another important consideration is the scalability⁵⁵ of the archiving solution, i.e. can the underlying infrastructure meet future requirements for the expected data load without the need of expensive redesign or implementation of completely new solutions?

To help to ensure long-term availability it is best to use platform independent (data) formats to archive business documentation electronically. If non-standard applications are used, special strategies to ensure continued availability should be developed⁵⁶.

Besides the archiving application(s) and the underlying infrastructure, the long-term availability of the storage media has to be considered. Physical measures to prevent the destruction or deterioration of storage media have to be taken, appropriate media types to be selected and a periodic check to ensure readability and data integrity to be performed. Additionally, to help to ensure availability, integrity and readability of the business documents for the whole archiving period, the process, or at least an approach for a possible migration, should be defined and documented. In this context, the validity of digital signatures and certificates has to be considered as well⁵⁷.

The existing security concept should be regularly updated. In order to control constantly changing IT threats, the implemented security technology should be adjusted to comply with up-to-date security and technology standards and best practices. Topics which

⁵³ ERNST & YOUNG, *Elektronische Archivierung*, 2007.

⁵⁴ ERNST & YOUNG, *Elektronische Archivierung*, 2007.

⁵⁵ "Scalability" is a desirable property of a system, a network, or a process, which indicates its ability to either handle growing amounts of work in a graceful manner, or to be readily enlarged.

⁵⁶ ERNST & YOUNG, *Elektronische Archivierung*, 2007.

⁵⁷ ERNST & YOUNG, *Elektronische Archivierung*, 2007.

should be considered are encryption technology, logical and physical protection of the information assets⁵⁸.

4 Consequences of non-compliant behaviour

What are the risks of non-compliant electronic archiving of records? What are the consequences if companies completely fail to comply with their legal obligation to properly keep and retain books of account? As mentioned above, if a company fails to observe its legal obligations regarding preservation of accounts and records and therefore lacks evidence that it has preserved its documents sufficiently, is to see its position in case of a legal dispute considerably weakened. In addition, the consequences of such non-compliant behavior can be costly. This is principally the risk from a civil law perspective or, if we take a larger view of the issue, this is a question of evidence. In my opinion, it is always better to be on the safe side.

Nevertheless, the consequences of complete failure to comply with a company's legal obligation to properly keep and retain accounting books can be very severe. From a penal point of view, Article 166 of the Swiss Penal Code (SPC) provide that a debtor who violates his legal obligation to regularly keep and preserve books or to prepare a balance sheet in such a manner that his financial situation is not or not completely transparent, shall be punished with imprisonment of maximum three years or a fine if he is declared bankrupt or if a loss certificate is issued against him following seizure of his assets, according to Article 43 of the Federal Act on Debt Enforcement and Bankruptcy of April 11, 1889.

The fact that the books were not kept in a proper manner, not done regularly or if the accounting and vouchers were not preserved is also considered failure to keep books⁵⁹. The debtor must be obligated to keep and retain books of accounts and he must intentionally fail to comply.

⁵⁸ ERNST & YOUNG, *Elektronische Archivierung*, 2007.

⁵⁹ Cour de cassation pénale, Decision 27 February 2006 ; SSC 77 IV 164 section. 1 page 166 ; SSC 117 IV 163 section 2b p. 165; CORBOZ BERNARD, *Les infractions en droit suisse*, vol. I, Berne 2002, n. 7, art. 166, page 496.

In addition, Article 325 SPC provide that :

a) whoever, intentionally or negligently, fails to comply with his legal obligation to properly keep books or

b) whoever, intentionally or negligently, fails to preserve books, business correspondence and telegrams,

shall be punished with a fine.

Article 325 SPC is only applicable if the requirements of Article 166 SPS are not fulfilled⁶⁰. Article 325 SPC punishes, contrary to Article 166 SPC, negligence as well as the intention to fail to comply with one's legal obligation to keep books.

In case the requirements of Article 166 SPS are fulfilled, the concerned person risks being punished with imprisonment of maximum three years or with a fine of maximum CHF 10'000⁶¹. If Article 325 SPC is applicable, the concerned person risks to be punished only with a fine of up to CHF 10'000⁶², which in my opinion is not really dissuasive.

In 2003 a new article was implemented into the Swiss Penal Code that punishes companies in a direct manner. Article 102 SPC provides that a crime or offence shall be attributed to the enterprise if committed during the course of exercising a business activity within the scope of the enterprise and if, due to the deficient organization of the enterprise, such act cannot be attributed to a natural person. In such a case, the enterprise can be punished with a fine of up to CHF 5 million. The final step in the pyramid of responsibilities for the preservation of documents is the board of directors (See Para 2.3 above). However, in my opinion it is unlikely that a failure to keep books or an irregular keeping of books, due to the deficient organization of the enterprise, cannot be attributed to a natural person. Therefore, the company itself has a smaller risk of being punished than the employee. Non-compliant behaviour can, therefore, have severe consequences for the responsible employees.

⁶⁰ Swiss Supreme Court (SSC) 72 IV 17, page 19; AMSTUTZ MARC / MANI REINERT, in: Basler Kommentar Strafgesetzbuch II Art. 111 – 401 StGB, Art. 325 StGB, page 2151.

⁶¹ Article 106 SPC.

⁶² Article 106 SPC.

5 Information Carriers

5.1 Permissible information carriers

Article 9 section 1 BRO provides that for the preservation of documents, the following information carriers are permissible: a) Unchangeable information carriers, in particular paper, picture carriers, and unchangeable data carriers; b) Changeable information carriers, if 1) Technical processes are used which ensure the integrity of the data stored (e.g. digital signature), 2) The time the data was stored can be correctly substantiated (e.g. by means of a “time stamp”), 3) The other provisions regarding the use of relevant technical processes in force at the time of storage are observed, and 4) The processes and the procedures for the use of information carriers are defined and documented and relevant ancillary information (such as protocols and log files) are also preserved.

As a basic principal, any media that ensures proper preservation (such as paper, image carrier, and unchangeable information carriers) can be used as an information carrier. The newness concerns the changeable information carriers, which are accepted if they fulfill the above mentioned conditions of Article 9 Section 1 BRO.

5.1.1 Unchangeable information carriers

Unchangeable information carriers do not constitute a major problem in practice. However, any modification or deletion on the data carrier has to be traceable, and the physical unfalsifiability has to be marked in order to identify it.

Unchangeable information carriers include e.g. CD-ROM (but not CD-R/W) or single-write DVDs. The main problem today with information stored on unchangeable information carriers is the durability of the information carriers themselves. Whilst the long-life music CDs and movie DVDs are machine pressed, the carrier material of a CD or DVD that one can write on is made of a chemical substance which is changed by the laser beam of the burner. The information carriers are susceptible to light and heat and the chemical substance deteriorates in the course of time, meaning that the information carriers eventually become unreadable. High-quality products stored under ideal conditions might remain readable for over 10 years. But the manufacturers offer no guarantees in this respect. In the cases we have seen of archiving on unchangeable information carriers, the carriers have been copied over to new information carriers every

two to five years. A similar thing applies for WORM storage solutions with the “Jukebox System”. In any case, the copying over must be recorded and the protocol must be retained together with the new information carriers (Article 10 Section 3 BRO)⁶³.

5.1.2 Changeable information carriers

According to Article 9 Section 2 BRO, information carriers will be classified as changeable if the data stored on them can be altered or deleted in a way that the alteration or deletion can not be recognized (e.g. magnetic tapes, magnetic or magneto-optical disks, fixed or removable disks, solid state memories).

As a matter of principle, a physically changeable information carrier with technically organized measures that reach the same level of immutability of unchangeable information carriers fulfills the “immutability” requirement set forth in Article 9 Section 1 BRO. The effectiveness of the used infrastructure is essential in order to make the difference between the two permissible information carriers. If the use of an information carrier with logical electronic writing block (so-called WORM⁶⁴) guarantees an appropriate organization of immutability, like a physically unchangeable information carrier (e.g. paper), the safety is the same. However, the equivalence has to be determined case by case.

The integrity and readability of the information on the data carrier should be regularly verified. Archived information has to be distinguished from the actual information. It should be possible to find the information within a useful period of time⁶⁵.

5.2 The four conditions of acceptance of the changeable information carriers

The changeable information carriers are admissible for the preservation of documents, as mentioned above, if the integrity of the data stored is ensured (Para 5.2.1), the time the data was stored can be correctly substantiated (Para 5.2.2), the other provisions regarding the use of relevant technical processes in force at the time of storage are observed, and the processes and the procedures for the use of information carriers are defined and

⁶³ ERNST & YOUNG, Legal News, January 2006 .

⁶⁴ WORM is an acronym for Write Once, Read Many, an optical disk technology that allows you to write data onto a disk just once. After that, the data is permanent and can be read any number of times. WORM is also called CD-R.

⁶⁵ See Paragraph 3.2.2. „Availability“ above.

documented and relevant ancillary information are also preserved (Para 5.2.3). This paper shall focus on the integrity of the recorded information and the time of record issue and especially the question of the electronic signature and the time stamp. These two topics give rise to the most questions in practice, especially concerning the type of certificate to use and who delivers time stamps. The last condition of acceptance of the changeable information carriers will be briefly set forth.

5.2.1 Integrity of the recorded information

As mentioned above, the integrity and readability of the information on the data carrier should be ensured. As of May 1, 2000 the Federal Council introduced the Ordinance on Services Related to Electronic Certification (OSREC) and as of January 1st, 2005 the Federal law on certification services (FCS) in the area of electronic signatures. The digital signature is a technical procedure which makes it possible to guarantee the authenticity of a document or an electronic message and to ensure the identity of the sender. It is based on a certification infrastructure managed by third party providers - the certification service providers. In order to encourage the development of e-commerce, the legislator allows such providers to be recognized on a voluntary basis. In addition, under certain conditions, the law assigns equal status to the electronic signature as to handwritten signatures⁶⁶. Therefore, digital signatures are able to minimize the fear of falsification⁶⁷.

The first purpose of the electronic signature is to secure that the information collected cannot be altered during their transmission (integrity). Secondly, it is important to assure that the information actually originated from the person who was meant to be the sender of the message (authentication). Third, it is crucial that already carried out information cannot be challenged and the information remains verifiable (non-repudiation). Finally, the same technology which provides digital signature also offers the possibility to encrypt the data (confidentiality)⁶⁸.

⁶⁶ Federal law on certification services (FCS); Communication, Federal Department of Justice and Police (FDJP), 06.07.2001 ; <http://www.ejpd.admin.ch/ejpd/fr/home/dokumentation/mi/2001/2001-07-06.html>; Message regarding the Federal law on certification services in the field of electronic signatures (ZertES); <http://www.admin.ch/ch/f/ff/2001/5423.pdf>.

⁶⁷ www.bakom.ch/themen/internet/00467/index.html?lang=fr.

⁶⁸ LEGLER THOMAS, *Electronic Commerce mit digitalen Signaturen in der Schweiz: Kurzkommentar zur Zertifizierungsdienstverordnung*, Bern, Stämpfl, 2001.

Literature describes in detail how a digital signature works⁶⁹. This paper will therefore limit itself to some central topics, i.e. a) Is a qualified certificate needed? b) Certification Authority (CA) and c) Foreign certificates.

a) Is a qualified certificate needed?

According to the FCS in the area of the electronic signature, a qualified certificate is understood as a digital certificate, which meets the conditions of Article 7 FCS. However, neither the BRO nor the 2005 Federal law on certification services in the area of the electronic signature mention whether a qualified certificate is needed in order to preserve documentation.

Concerning the issue of qualified certificates (Article 5 of the Decree on certification services in the area of the electronic signature and Article 8 of the Federal law on certification services in the area of the electronic signature), a recognized certification service provider must oblige persons requesting a qualified certificate to personally present an identity card or a passport.

They must also require persons who have specific attributes to present the documents proving these attributes, such as, for example, a power of attorney. Insofar as the specific attributes refer to an entry in the commercial register, the following documents must also be presented: a) Current certified extract from the commercial register; b) Statement of acceptance:

- of the holder, in the case of an individual undertaking;
- of the associates, in the case of a company of persons;
- of the highest management or administration body, in the case of a legal entity.

Recognized certification service providers may accept a request accompanied by a qualified electronic signature when a person without specific attributes and identified in accordance with Section 1 of Article 5 of FCS less than six years previously requests a new qualified certificate.

⁶⁹ SCHLAURI.

Article 7 of the Decree on certification services in the area of the electronic signature (DFCS) provides that recognized providers shall inform their clients of the manner of requesting revocation of qualified certificates. They must guarantee third-party online access to the information relating to the revocation of a qualified certificate up to the expiry of the latter's validity. Recognized certification service providers must be able to provide the information enabling verification of qualified certificates which are no longer valid for eleven years from the expiry of the certificates.

Concerning the Security measures (Article 11 DFCS), the holder of a qualified certificate must not entrust the signature-creation device to anyone else. To the extent that it may be required, the holder must keep this device in its possession or place it in a secure location. In the event of loss or theft of the signature-creation device, the holder of a qualified certificate must request revocation of the latter within the shortest possible time. The same applies to a holder who knows or has reason to believe that a third party may have had access to the signature key.

As showed above the provisions to fulfill and the consequences in case of a qualified certificate are many. However, I recommend always proceeding to this kind of certificate, because of two main reasons: In addition to the above mentioned commercial provisions of the CO and the BRO, there are a number of other special provisions concerning preservation of documents. The ordinance on the VAT Act (VATAO), the Ordinance about electronically transferred data and information (OEIDI) and the Ordinance on Services Related to Electronic Certification (OSREC) are also of great importance (see Para 6. Special cases). This regulation concerning tax law provides that a qualified certificate is needed. It seems logical to adopt a harmonized model and apply the qualified certificate model to any documents that have to be preserved. The second reason for recommending a qualified certificate is an evidence reason: if the integrity of a document has been ensured by a qualified certificate in the sense of Article 7 FCS the integrity of the document may not easily be challenged by a third party and in a legal dispute the burden of proof that the document has not be changed is on the other side. This puts the company in an advantageous position compared the other party. If the company uses ordinary certificates, the above-mentioned burden of proof is on the company's side. This can be even more costly than implementing immediately qualified certificates.

b) Certification Authority (CA) and Certification Service Providers

In order to certify that the identity of each user corresponds with her/his digital signature, a trusted third party is needed. This third party, a Certification Authority (CA), will authenticate signatures as belonging to a specific user through the provision of a digital certificate. It is the role of these mostly privately owned providers and their infrastructure (Public Key Infrastructure, PKI) to set up, issue and manage digital signatures as well as certificates in compliance with the DFCS⁷⁰.

For certification authorities who are referred to as Certification Service Providers, the DFCS provides the possibility of receiving a sort of seal of approval. For this purpose, a voluntary system for recognition is provided based on the Federal Law on Technical and Commercial Barriers to Trade and the Ordinance for Accreditation and Designation (Akkreditierungs- und Bezeichnungsverordnung, AkkBV). The provider will be recognized by a certification Body (CB) that will be accredited by the Swiss Authority for Accreditation (SAS)⁷¹ of the Swiss Office of Measurements. In absence of CB, the SAS, which takes on the role of supervisory body, will directly certify the providers⁷². Each certified provider is added to a publicly accessible list kept by the SAS. In order for a provider to be certified by the authorities he must fulfill the various conditions stipulated in the DFCS. These include, e.g., qualified staff, reliable IT material and sufficient finances. In addition, the provider must agree to abide by the applicable laws.

At the moment only KPMG exists as a certification body (CB):

KPMG Klynveld Peat, (Marwick Goerdeler SA, ISMS Zertifizierungsstelle, SCESm 071, Badenerstrasse 172, 8026 Zürich 4, SWITZERLAND).

Directory of the Certification Service Providers conform to the Federal law on certification services (FCS)⁷³:

⁷⁰ LEGLER.

⁷¹ www.seco.admin.ch/sas/index.html?lang=fr.

⁷² www.seco.admin.ch/php/modules/service/popup.html?lang=en&bild=NHZLpZag7t,lnJ6IzdeIp96km56VIWRpnJIOqdayXbGH7IuqtJ_o.

⁷³ www.seco.admin.ch/sas/00229/00251/00253/index.html?lang=en;
www.seco.admin.ch/sas/00229/00251/00254/index.html?lang=en;
www.seco.admin.ch/sas/00229/00251/00281/index.html?lang=en.

Certification Service Providers	Certification Date
Swisscom Solutions AG Lindenpark 1, 3048 Worblaufen SWITZERLAND	December 2, 2005
QuoVadis Trustlink Schweiz AG Brügglistr. 2, 8852 Altendorf SWITZERLAND	April 13, 2006
SwissSign AG Beethovenstrasse 49, 8002 Zürich SWITZERLAND	October 30, 2006

Concerning the liability of providers, Article 16 FCS provides that it is their responsibility to provide proof that they have complied with the obligations deriving from the present law and the implementing provisions. Providers cannot exclude their liability deriving from the FCS nor that of their auxiliaries. However, they are not liable for damage resulting from non-compliance with or violation of a restriction on the use of the certificate (Article 7 Section 2 FCS).

Concerning the liability of recognition bodies Article 17 FCS provides that they are liable for the damage caused to the holder of the signature key and to third parties, which have trusted a valid qualified certificate.

c) *Foreign certificates*

The European Union has enforced a Directive for Digital Signature⁷⁴ which provides that each Member State adopt the necessary corresponding national provisions before 19 July 2001. According to Article 5 of the EU Directive (Legal effects of electronic signatures), Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and b) are admissible as evidence in legal proceedings.

Article 5 Section 2 states that an ordinary certificate can be admissible as evidence in a legal proceeding. Thus, even in the EU Community a qualified certificate is not obligatory. However I recommend the qualified certificate for the reasons mentioned in Para 5.2.1a). and because the recognition of a foreign certificate will be easier if the certificate is a qualified one.

Germany, Italy, Austria, Spain and other countries belonging to the European Community have already enacted national legislations on this issue.

Over 40 States in the USA have also introduced corresponding laws, and President Clinton had signed the Federal Electronic Signature in Global and National Commerce Act⁷⁵. Finally, also international organizations such the OECD or UNICITRAL are preparing regulations. In this respect, the Ordinance on Services Related to Electronic Certification provides in Article 1 OSREC, the international recognition of certification authorities and their services.

5.2.2 Time of record

Concerning the time-stamping system, Article 12 FCS stipulates that recognized providers shall issue, on request, a statement accompanied by their qualified electronic signature for the purposes of establishing the existence of digital data at a precise point in time.

A certified time stamp is a digital code (bit pattern), which is generated by specific software and hardware. It identifies the time when a document is digitally filed (digital

⁷⁴ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

⁷⁵ www.ftc.gov/os/2001/06/esign7.htm.

archiving). The use of a certified time stamp is in conformance with standardization and fully complies with the legal requirements (BRO, OEIDI) in Switzerland⁷⁶.

Time is also a key factor for purposes of commercial law and tax law. Under commercial law (BRO), proof of the integrity of the time indicating when the information was filed is required, and under tax law, electronic signatures must always be examined before the electronically signed data are used, and authenticity must be documented.

Using a certified time stamp that ties together a reliable point in time and the document or activity meets the requirements of both commercial and tax law.

Since July 2006, KPMG has been accredited to certify companies wishing to take advantage of the benefits of an internal time stamp service in accordance with international standards. At the same time, KPMG is the only certification body for time stamps in Switzerland⁷⁷ and the certification service providers are the same as for the qualified certificates (see Para 5.2.1b)).

This ensures the legal certainty of a secure, reliable time stamp, which is in compliance with commercial law and tax law.

To be reliable, the time-stamps must not be forgeable. Consider the requirements for a digital time-stamping service of the type just described:

The digital time-stamping service itself must have a long key if we want the time-stamps to be reliable for, say, several decades. The private key of the digital time-stamping service must be stored with utmost security, as in a tamperproof box.

The date and time must come from a clock, also inside the tamperproof box, which cannot be reset and which will keep accurate time for years or perhaps for decades. It must be infeasible to create time-stamps without using the apparatus in the tamperproof box.

The use of a digital time-stamping service would appear to be extremely important, if not essential, for maintaining the validity of documents over many years. In addition to that, I strongly recommend using such a time stamp, because of the reason mentioned in Para

⁷⁶ KPMG, in : Media Release Zurich, 15 August 2006 ;

http://www.kpmg.ch/library/pdf/Media_Release_Zertifizierung_Zeitstempel_DES.pdf.

⁷⁷ GRUBENMANN RETO, Head of the Certification Office, Information Risk Management, KPMG Switzerland.

4.2.1 a): The integrity of the document cannot easily be challenged by a third party and in a legal dispute the burden of proof that the document has not been changed, is carried by the other party. The time stamp, cumulated with the qualified certificate, puts the company in a strong position.

5.2.3 Compliance with the provisions regarding the use of technical processes at the time of storage and documentation of the processes and procedure for the use of information carriers

Companies are free to choose the relevant technical process they want to use for the storage. This paper explained above (see Para 5.2.1 and 5.2.2) the possibility offered by the electronic signature and the time stamp. Even if those two technical processes require the compliance of more provisions, I recommend them. Indeed, as mentioned above, the integrity and the point in time of the document may not easily be challenged by a third party and in a legal dispute the burden of proof that the document has not be changed is on the other side. If the company technical process, which no third trusted party (such as a Certificate Service Provider) has delivered, the burden of proof is carried by the other party. This can be even more costly than immediately implementing qualified certificates and time stamps.

Companies must, however, comply with the provisions of this technical process at the time of storage. The “time of storage” is of significance. If the provisions change, the company fulfills this condition in proving that, at the time of storage, it was in compliance with the provisions. This is an additional argument to request a qualified certificate or a time stamp from a third trusted party: If the provisions at the time of storage were not fulfilled, the qualified certificate or the time stamp would have been denied.

In a second time, the processes and the procedure chosen for the use of information carriers have to be defined and documented and the relevant ancillary information (such as protocols and log files) have also to be preserved.

5.3 Data migration and examination

Article 10 BRO provides that the information carriers should be inspected regularly regarding their integrity and readability. The data can be transferred to other formats or to other information carriers (so-called data migration), if it is ensured that: a) The completeness and the accurateness of the information remain guaranteed; and b) The

availability and the readability further comply with the legal requirements. Minutes shall be taken of the transfer of the data from one information carrier to another. The minutes shall be preserved together with the information.

As a matter of fact, some information has to be, from time to time, transferred on other information carriers, because the actual data format or the engaged storage media do not guarantee the required readability anymore or because new storage media are available. The readability must be ensured at all times.

Paper-based information can e.g. be imported with a so-called scanner. This electronic information can then be passed on in the same manner as the scanner importation. As long as there is no special provision stipulating that the document has to be absolutely preserved in the original format, the information can be “theoretically” (see Para 2.6 and especially Para 2.6.1) preserved in the electronic form with this scanner importation procedure⁷⁸. The paper-based information does not have to be preserved in addition to the electronic one. Another special case concerns the dismissal of objection, which will be discussed in Para 6 “Special cases”.

⁷⁸ BELINGER / LEHMANN / NEUENSCHWANDER / WILDHABER, page 131 et seq.

6 Special cases

As mentioned in the Para above, there are a number of other special provisions concerning preservation of documents. The Ordinance on the VAT Act (VATAO), the Ordinance about electronically transferred data and information (OEIDI) and the Ordinance on Services Related to Electronic Certification (OSREC) stipulate special provisions concerning VAT and income tax, especially regarding the preservation period. In addition, the cases of loss certificate and dismissal of objection will be briefly discussed.

6.1 VAT

The Federal Tax Administration (FTA), for instance, has laid out a set of rules that must be considered whenever invoices including VAT are transmitted and stored electronically (OEIDI). These rules are even stricter and more specific than those found in the BRO⁷⁹.

With regard to the VAT the two following cases have to be distinguished:

- a) Transmission of data in hard-copy and
- b) Electronic data transmission.

When hard-copies are covered into electronic format (e.g. by scanning invoices) or when the documents exist in hard-copy as well as in electronic form (e.g. turnover reconciliations), the BRO provisions must be complied with in addition to the VAT Act⁸⁰, the VATAO, as well as the OEIDI provisions and the 2001 Instructions on VAT⁸¹.

The OEIDI and the OSREC only apply in case of preservation of electronically generated and transferred or received data. This primarily includes all documents that are relevant for the input tax deduction, the calculation of the VAT due and the levying of the tax. Electronically transferred or received and archived VAT-relevant data only possess

⁷⁹ <http://www.homburger.ch/fileadmin/publications/DRRPPITD.pdf>.

⁸⁰ http://www.kpmg.ch/library/pdf/20031202_KPMG_Tax_MWSTG_E.pdf.

⁸¹ <http://www.estv.admin.ch/f/mwst/dokumentation/publikationen/pdf/610.525f.pdf>.

probative force as required by VAT Act if they are secured by a digital signature (Article 43 section 1 VATAO in connection with Article 3 Section 1, letter a OEIDI)⁸²:

The conditions for evidential value required in Article 43 Section 1 VATAO are fulfilled if:

- The transmission and storage of data is ensured using digital signature. Digital signature refers only to signatures which a) are based on a certificate issued in accordance with the provision of the OSREC; b) are based on a certificate originating from a accredited certification service provider under Article 3 et seq. FCS; and c) are produced with means over which the owner alone is able to exercise sole control.
- The certificate issued by a certification service provider under Article 3 et seq. FCS, was valid at the time at which the signature was established.
- The electronic data is checked before use by means of digital signature verification with respect to integrity, authenticity and signature authorization and the result documented;
- The public key needed to check the digital signature is kept with the secured data; this also applies for certificates issued by an accredited certification service provider in so far as the certificates have not been published.
- On application of encryption tools the key to decode encrypted data is retained.
- No pseudonyms are used.
- The keys may beyond doubt be considered as secure at time of use.

Electronically transmitted data that the recipient sends to the address of the supplier (e.g. credit note) or that he generates in the name of and for the account of the supplier (self-billing) require an acknowledgment of receipt by the supplier. This must fulfill the above mentioned conditions and make clear reference to the data received⁸³.

⁸² BELINGER / LEHMANN / NEUENSCHWANDER / WILDHABER, page 134.

⁸³ BELINGER / LEHMANN / NEUENSCHWANDER / WILDHABER, page 134.

This kind of acknowledgment of receipt is also required if the supplier wishes to provide proof that the recipient has his place of business or residence abroad on the basis of electronically transmitted data alone.

Concerning the data security, OEIDI rules provide that the data processing procedure applied must provide assurance that all of the data which is to be processed and could be required for tax collection purposes is captured and in addition cannot be suppressed or altered unnoticed. All records of data and data processing systems which may be relevant for tax purposes and corresponding checks by the FTA⁸⁴ must be protected by means of systematic directories and adequate access controls to data and premises against disappearance, unauthorized changes, destruction and theft (Article 4)⁸⁵.

A procedural record must be made for every data processing system (e.g. accounting system). The size and structure of this procedural record should be designed in such a manner that a third person with knowledge of bookkeeping is able to understand how the data processing system operates for which it was created without additional explanation. Master files and (steering) tables must be documented. The lifespan of entries and any amendments thereof must be retained and commented. It must also be ensured that they can be reproduced legibly without unreasonable delay. The use of numerical order and codes is exclusively permitted for article designation and requires that their meaning is clear and may be determined without unreasonable delay by the sender as well as by the recipient of data. The condition of verifiability is therefore very similar to the BRO^{86, 87}. It makes sense to have a uniform system, even if it is not obligatory for accounting documents to fulfill all these strict provisions. However, it is always better to be on the safe side and, if these conditions are followed for the entire business-relevant documentation, any transaction can be proven in case of a dispute.

Taxpayers must ensure that the relevant data required for tax collection purposes and the working instructions and other organizational documents necessary for their comprehension such as table settings are readable without unreasonable delay. Moreover,

⁸⁴ <http://www.estv.admin.ch/f/index.php>.

⁸⁵ EGGER KARL / NIEDERBERGER MARCEL, in: Der Schweizer Treuhänder 6-7/02, *Elektronische Übermittlung und Aufbewahrung von für die MWST-Erhebung relevanten Daten*, 2002.

⁸⁶ BODMER THOMAS, in : Der Schweizer Treuhänder 6-7/04, *Elektronischer Geschäftsverkehr und MWST – Risiken für Anwender nicht ausgeschlossen*, 2004.

⁸⁷ MEYER CHRISTOPH, in : Der Schweizer Treuhänder 6-7/01, *Rechtliche Probleme der elektronischen Datenaufbewahrung – Zulässigkeit, Aufbewahrungsdauer*, 2004, 587 et seq., 590.

they are obliged to provide all necessary documents for their comprehension and if necessary furnish reproductions of the documents that are readable without the need for other aids. In addition, data stored for tax collection purposes must be presented unchanged and complete when reproduced as well as easily comprehensible (Article 6).

Because the FTA is authorized to inspect on site any stored data relevant for tax collection purposes, the taxpayer must take all necessary precautions to ensure that data access does not result in data being altered or any other damage occurring to its data processing systems. The consequences of not fulfilling such diligence obligations shall be borne solely by the taxpayer concerned⁸⁸.

It must be possible to check each commercial operation individually at all stages from the accounting voucher to the accounting books and from there to the VAT statement without unreasonable delay or significant cost and in the other direction. Archiving, any eventual conversions and other operations must be recorded in a protocol.

Moreover, electronic data relevant for tax collection purposes must be stored by the sender and the recipient in the original form in which it was transferred and in its entirety on data carriers capable of automated processing. Storage exclusively in printed form or on micro-film is not permitted. When converting data relevant for tax collection purposes into another format (in-house format), both versions must be stored and recorded with the same index. The converted version must be marked accordingly. The storage of data carriers abroad is only permissible if access, readability and evaluation of the data relevant for tax collection purposes can still be assured at all times.

Finally the duration of storage and deletion of electronic data relevant for tax collection purposes is subject to the provision of Article 58 Section 2 of the VAT Act, i.e. the taxable person is obliged to keep his or her books of account, vouchers, business papers and other records in an orderly fashion for a period of ten years. Article 962 Section 2 CO remains under reserve. The business documents associated with immovable property are, however, to be kept for 20 years. If, after expiry of the storage period, a tax claim which relates to the books of account, vouchers, business papers and other records has not yet lapsed, the storage obligation continues until the statute of limitations is reached.

⁸⁸ OBERSON XAVIER, in : Der Schweizer Treuhänder 09/99, *Le commerce électronique et la TVA*, 1999.

Companies therefore have to deal with longer preservation periods regarding the tax aspect.

If these rules are not observed, a VAT-taxable company receiving an invoice may not be allowed to deduct the VAT it paid to its subcontractor on its own VAT return. Depending on the circumstances, this can ruin a business. Nevertheless, many companies will find that compliance with the rules on electronic invoices set forth by the VAT administration is not worthwhile. In such cases paper-based invoices will have to be used, even if the underlying transaction takes place electronically. Businesses should not accept invoices that are provided by electronic means only, such as by email or as web-pages. Companies that offer services or goods to businesses in Switzerland should be aware of these restrictions as well.

However the Federal Tax Administration continually monitors the latest technical developments in the transfer and storage of electronic data relevant for tax collection purposes. It fosters the necessary contacts with leading active users of these technologies with a view to being able to identify any necessary adoption to latest standards in information technology.

This well organized procedure concerning VAT-relevant data does, according to my point of view, completely lack for the other documents discussed in Para 2 above. As a matter of fact, it is difficult to find out how a qualified certificate for non-VAT documents has to be established. The Certification Authority and the Certifications Service Providers should, in my opinion, set up a procedure based on the VAT one, in order to allow companies to establish a qualified certificate. It is vain to allow qualified certificates for non-VAT documents, if no easy findable procedure to obtain this kind of certificate is provided.

6.2 Income Tax

The principle that tax accounting should be based on commercial accounting is applicable in all matters regarding income tax. Accounting books that have been preserved in accordance with the imperative provisions of Swiss commercial law are relevant for all

such matters. The CO and the BRO therefore also apply to the assessment of the archiving system with regard to income tax matters⁸⁹.

According to Article 120 of the Federal Income Tax Statute (FITS) regarding the statute of limitation of the right to assess taxes, the right to assess taxes is barred by the statute of limitation to five years after the expiration of the tax period. Article 152 and 184 are reserved. The right to assess taxes is in any case barred by the statute of limitation to 15 years after the expiration of the tax period.

Regarding the statute of limitation of the right to levy taxes, tax claims are barred by the statute of limitation to five years after the assessment became binding. In any case, the statute of limitation occurs ten years after expiration of the year in which the tax assessment became binding.

There is an additional obligation to co-operate: The person liable to tax must do anything in order to enable a complete and correct assessment. Upon request, he/she must provide verbal or written information, books of account, vouchers, and further certificates as well as deeds concerning the business volume to the tax authority. Legal entities must record books of account and schedules according to Article 125 Section 2 FITS and other vouchers relating to their activity for ten years. The manner of keeping, recording and editing complies with the provisions of Article 957 and 963 Section 2 CO.

The right to initiate a supplementary tax proceeding for which an assessment was omitted wrongfully or a final assessment was incomplete expires ten years after the expiration of the tax period. The right to assess supplementary taxes is barred by the statute of limitation to 15 years after the expiration of the tax relevant period.

6.3 Recognition of Debt

A claim for money may be enforced more easily during debt collection proceedings (setting aside any objections) if it is based on a recognition of debt contained in a signed document. Thanks to the recognition of the electronic signature as equivalent to a handwritten signature, the use of electronically signed digital recognitions of debt (e.g. contained in an e-mail) is now possible. It is, however, necessary for the courts to have

⁸⁹ ERNST & YOUNG, *Elektronische Archivierung*, 2007.

the adequate means of technology to allow verification⁹⁰. The extent to which courts will be equipped with such technology has not yet been determined and this is, in my opinion, regrettable. Courts should start to enclose current technology, because with the adequate means and training, such technology could be of precious help in cutting down on time .

6.4 Dismissal of objection

The objection is dismissed if the creditor shows that the debtor actually owes the debt. The dismissal of objection can be either final (Article 80 Federal law on Debt collection and Insolvency, FDI) or provisional (Article 82 FDI). If a definite objection of dismissal is requested, a court decision is required, while a provisional requires a recognition of debt (see Para 6.3 above). The latter could be in electronic format. It is, nevertheless, better to preserve the paper-based original of the recognition of debt, because as written above, it has not been determined to which extent the courts will be equipped with the adequate technology to allow verification. In addition, GASSER and HÄUSERMANN⁹¹ explain that, because no court decision regarding the electronically signed digital recognitions of debt exists, court decisions regarding photocopies of recognitions of debt are applicable. Cantonal courts have taken non-uniform decisions about this issue. A photocopy of a recognition debt is accepted by some courts⁹², others require that the debtor accepts the photocopy as being identical to the original. MAYER⁹³ recommends preserving the original in addition to the electronic copy in any case since no clear practice has been established. In my opinion, it is time that the legislator clarifies this issue. It is not admissible to wait a court decision, which is in any case not binding for the other courts. In addition to that, the second step will be to provide the adequate means and training of the staff in order to enclose present-day technology and make this latter efficient.

⁹⁰ SCHELLENBERG WITTMER AVOCATS.

⁹¹ GASSER/HÄUSERMANN.

⁹² St.Gallen, Thurgau, Argau, Uri, Basel-Land, Luzern, Neuburg, Waadt and Graubünden.

⁹³ MEIER, 587 et seq., 590.

6.5 Audit Supervision Act and Article 730c CO

In 2004, the Message regarding the legal requirements relating to audits⁹⁴ issued several amendments to the Swiss Code of Obligations and the Audit Supervision Act (ASA). The project of the new ASA should come into force in the second half of 2007 or in the beginning of 2008. This law has emerged in the light of the more rigorous requirements that are now in force in US legislation and will simplify international cooperation in this area.

The old as well as the new ASA also requires the documentation and preservation of audit documents. Article 13 new ASA provides that state supervised auditors⁹⁵ shall protocol all the services provided and preserve all the audit reports and all the significant documents for a period of ten years. The access to the information recorded on an information carrier shall be ensured during this ten years-period of time. Contrary to Article 962 CO (See Para 2.4), the start of the preservation period is the storage date of the document. In addition all audit reports, as well as the working papers (internal papers), have to be preserved. The documents have to be dated and have to mention the author and the auditor responsible of the mandate^{96, 97}. These additional requirements are justified not only because they ensure internal quality, but especially because they allow the supervisory authority to easily check if the auditor respects the legal provisions⁹⁸. Furthermore, it can always be evidence in case of a legal dispute.

In addition to the ASA, the proposed⁹⁹ Article 730c, that has the same content as Article 13 ASA¹⁰⁰, was accepted by the National Council in 2005¹⁰¹. LEUTENEGGER OBERHOLZER explains the necessity to have this preservation requirement in the Swiss Code of

⁹⁴ Message regarding the amendments of the Swiss Code of Obligations (legal requirements relating to audits) and the Audit Supervision Act (ASA), 23 June 2004.

⁹⁵ Auditors of publicly held companies are subject to state supervision and are reviewed by the supervisory authority at least every three years.

⁹⁶ Message regarding the amendments of the Swiss Code of Obligations (legal requirements relating to audits) and the Audit Supervision Act (ASA), 23 June 2004, Article 13 ASA.

⁹⁷ LEUTENEGGER OBERHOLZER states that the date and the name of the author are from a practical point of view sufficient, *Conseil National*, Spring Session 2005, Fourth session, 2 March 2005 (15h).

⁹⁸ Article 17 ASA Control of the state supervised auditors.

⁹⁹ By the Commission charged by the FTA.

¹⁰⁰ IMFELD ADRIAN, *Neuregelung der Revision vor der Beratung im Nationalrat*, in: *Der Schweizer Treuhänder* 3/05, page 127.

¹⁰¹ *Conseil National*, Spring Session 2005, Fourth session, 2 March 2005 (15h);

http://www.parlament.ch/ab/frame/frameset/f/n/4707/119238/f_n_4707_119238_119239.htm.

Obligation and not only in the ASA in the name of the Commission. Hence, all enterprises have to comply with this preservation requirement and not only the enterprises covered by the ASA.

6.6 Personal records

The issue of data proper to retired or resigned employees constitutes the last special case discussed in this paper. From a data protection point of view there may be a problem regarding the preservation of these personal data after the retirement or resignation of the employee. According to the Federal Data Protection and Information Commissioner (FDPIC)¹⁰² there is an overriding interest of the employee¹⁰³ that those records, such as performance information, are deleted after his retirement or resignation as opposed to the legal obligation of the company to keep and retain documents. FDPIC provide the deletion of these personal data usually after five years. The deletion of personal data in electronic format are, however, not always possible. The personal data shall in this case be overwritten, in order to avoid any violation of the employee's private sphere.

¹⁰² Federal Data Protection and Information Commissioner (FDPIC), *Guideline regarding personal data at work*; <http://www.edoeb.admin.ch/index.html?lang=en>.

¹⁰³ <http://www.edoeb.admin.ch/dokumentation/00445/00472/00535/index.html?lang=fr>.

7 Conclusion

Although Switzerland has established a fairly comprehensive legal framework regarding electronic preservation of documents, it still is missing clear guidelines for companies and a uniform practice. The existing preservation regulations that were enacted during the past few years and that aim for regulation of document preservation (including documents in electronic format), are still of a rather preliminary nature. Many questions are left unresolved for the parties concerned: Is, for example, a qualified certificate or a time stamp provided by a trusted third party necessary in order to fulfill the legal requirements?

In addition, the requirements regarding preservation differ depending on the type of document (accounting, tax or audit document). It takes time for companies to establish an organized and secure system of document preservation that fulfills all the different legal obligations. Companies, however, have an interest, especially from a probative point of view, in retaining as many documents as possible - without breaching data protection principles - in their written and signed ("original") form.

The probative force of an electronic copy differs, indeed, in several factors (type of documents copied or Cantonal Court, for example). By retaining documents in original form, companies avoid lacking evidence, which may weaken their position considerably in the case of a legal dispute. The consequences of a lack of evidence can be very costly.

Moreover the consequences of non-compliant behavior can be grave, especially for the responsible employees: The latter risk being punished with imprisonment of a maximum of three years or with a fine of up to CHF 10'000 if he fails to keep books. The company itself also risks being punished with a fine of up to CHF 5 million if, due to deficient organization of the enterprise, the failure cannot be attributed to a specific employee.

In any event, the implementation of an organized and secure system is surely recommendable. Even if such implementation requires time, it certainly helps to prevent companies from suffering costly and severe consequences that can arise from insufficient or lack of correct document preservation.

Abbreviations

AkkBV	Ordinance for Accreditation and Designation
ASA	Audit Supervision Act
BRO	Business Record Ordinance
CB	Certification Body
CC	Swiss Civil Code
CO	Swiss Code of Obligations
DFCS	Decree on Certification services in the area of the electronic signature
FCS	Federal law on Certification Services
FDI	Federal law on Debt collection and Insolvency
FDP	Federal law on Data Protection
FF	Feuille Fédérale
FITS	Federal Income Tax Statute
FTA	Federal Tax Administration
OEIDI	Ordinance on Electronically Transmitted Data and Information
OSREC	Ordinance on Service Related to Electronic Certification
SAS	Swiss Authority for Accreditation
SPC	Swiss Penal Code
SSC	Swiss Supreme Court
VATA	Value Added Tax Act
VATAO	Ordinance on the Value Added Tax Act

Bibliography

ABAKUS, *Elektronische Archivierung – Gesetzlich Anerkannt*, 2002;
www.abacus.ch/downloads/pages/2002-03/s18-23.pdf

Administration fédérale des contributions AFC, *Instructions 2001 sur la TVA* ;
<http://www.estv.admin.ch/f/mwst/dokumentation/publikationen/pdf/610.525f.pdf>

AMSTUTZ MARC / MANI REINERT, in: Basler Kommentar Strafgesetzbuch II Art. 111 – 401
StGB, Art. 325 StGB

BELINGER JACQUES / LEHMANN BEAT / NEUENSCHWANDER PETER / WILDHABER BRUNO,
Records management, Leitfaden zur Compliance bei Aufbewahrung von elektronischen
Dokumenten in Wirtschaft und Verwaltung mit Checklisten, Mustern und Vorlagen, 2004

BLIGGENSTORFER SIMON, *Records Management*, Individual Assignment Paper CIB_01/06,
Private Hochschule für Wirtschaft, 12 February 2007

BODMER THOMAS, in : Der Schweizer Treuhänder 6-7/04, *Elektronischer Geschäftsverkehr
und MWST – Risiken für Anwender nicht ausgeschlossen*, 2004

BOSSARD ERNST, in: Zürcher Kommentar, *Die kaufmännische Buchführung*, Artikel 957-
964 OR, Teilband V/6/3b

BÜHLER ALFRED, „Die Beweiswürdigung“, in: Christoph Leuenberger (Hrsg.), *Der Beweis
im Zivilprozess*, Bern 2000

CALMES JEAN-CHRISTOPHE, Question de droit, in : La question du jour de l’OAV, *De
l’archivage électronique*, juillet-août 1999 ; www.oav.ch/Question/07_08_99.html

CORBOZ BERNARD, *Les infractions en droit suisse*, vol. I, Berne 2002

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

EGGER KARL / NIEDERBERGER MARCEL, in: *Der Schweizer Treuhänder* 6-7/02, *Elektronische Übermittlung und Aufbewahrung von für die MWST-Erhebung relevanten Daten*, 2002

ERNST & YOUNG, *Elektronische Archivierung*, 2007

ERNST & YOUNG, in : Legal News, *L'ordonnance concernant la tenue et la conservation des livres de comptes en pratique*, January 2006 ;

http://www.comptaval.ch/backoffice/images/newsfichiers/newsFichier_142.pdf

Federal Data Protection and Information Commissioner (FDPIC), *Guideline regarding personal data at work*; <http://www.edoeb.admin.ch/index.html?lang=en>

FORSTMOSER PETER / SPADIN MARCO, *Entwicklungen im Gesellschaftsrecht (Handelsgesellschaften und Genossenschaften) und im Wertpapierrecht*, (Erweiterte Fassung des in SJZ 101 [2005] Nr. 21 499 ff. publizierten Beitrages), 2006;

http://rwiweb.uzh.ch/forstmoser/publikationen/pdfdok/Entwicklungen_051025_Internetversion_clean.pdf

GASSER URS / HÄUSERMANN DANIEL MARKUS, in : *Beweisrechtlich Hindernisse bei der Digitalisierung von Unternehmensinformationen*, AJP/PJA 3/2006

GOVERNANCE INSTITUTE, COBIT 4.0, *The newest evolution of Control Objective and related Technology, the world's leading IT control and governance framework* (www.itgi.org and www.isaca.org/cobit)

GRUBENMANN RETO, Head of the Certification Office, Information Risk Management, KPMG Switzerland

HAYWARD DENISE, in: *Archives et législation*, 2005

HOMBURGER, in : Information Technology – Switzerland, *Data retention requirements pose problems for IT departments*, 2 September 2003 ;

<http://www.homburger.ch/fileadmin/publications/DRRPPITD.pdf>

IMFELD ADRIAN, *Neuregelung der Revision vor der Beratung im Nationalrat*, in: *Der Schweizer Treuhänder* 3/05

KÄFER KARL, in: *Berner Kommentar, Die kaufmännische Buchführung*, Artikel 957 OR

KPMG, in : Media Release Zurich, 15 August 2006 ;

http://www.kpmg.ch/library/pdf/Media_Release_Zertifizierung_Zeitstempel_DES.pdf

KOSTKIEWICZ / BERTSCHINGER / BREITSCHMID / SCHWANDER, in : *Handbuch zum OR*, Zürich, 2002

LEGLER THOMAS, *Electronic Commerce mit digitalen Signaturen in der Schweiz: Kurzkomentar zur Zertifizierungsdienstverordnung*, Bern, Stämpfl, 2001

LEUTENEGGER OBERHOLZER in : *Conseil National, Spring Session 2005, Fourth session* , 2 March 2005 (15h)

Message regarding the revision of the heading thirty-two of the Swiss Code of Obligations, 31 March 1999 ; <http://www.admin.ch/ch/f/ff/1999/4753.pdf>

Message regarding the amendments of the Swiss Code of Obligations (legal requirements relating to audits) and the Audit Supervision Act (ASA), 23 June 2004

Message regarding the Federal law on certification services in the field of electronic signatures (ZertES); <http://www.admin.ch/ch/f/ff/2001/5423.pdf>

MEYER CHRISTOPH, in : *Der Schweizer Treuhänder* 6-7/01, *Rechtliche Probleme der elektronischen Datenaufbewahrung – Zulässigkeit, Aufbewahrungsdauer*, 2004

NEUHAUS MARKUS / BINZ PETER, in: Kommentar zum Schweizerischen Privatrecht, Obligationsrecht II, Basel/Frankfurt a.M., 2002

OBERSON XAVIER, in : Der Schweizer Treuhänder 09/99, *Le commerce électronique et la TVA*, 1999

SCHELLENBERG WITTMER AVOCATS, in : Newsletter, *Les données électroniques dans le monde des affaires: une nouvelle loi et des développements récents*, April 2005;
http://www.swlegal.ch/downloads/newsletters/SWnews_0405F.pdf

SCHLAURI SIMON, *Elektronische Signatures*, Zürich 2002

SCHNURRENBERGER CATHRIN, *Datenaufbewahrungspflicht – ein Minenfeld für den VR*;
<http://www.itandlaw.ch/html/set/publikationen.html>

Schweizer Handbuch der Wirtschaftsprüfung, Treuhand-Kammer,
Zürich, 1998

UNCITRAL Model Law on Electronic Commerce Guide to Enactment with 1996 with
additional article 5 as adopted in 1998bis

WUERGLER RAOUL OLIVIER, in : Banque & Finance, *Une chaîne de haute sécurité pour les données sensibles*, Septembre – Octobre 2006

Acknowledgement

Firstly I express my sincere thanks to Professor Peter who has helped me in my studies at Geneva University and provided guidance with the writing of this paper. I also thank all the other professors and staff in the MBL program who have provided kind assistance and support during my stay at the University.

Secondly, I thank Mr. Krohmann, who was the responsible person in Ernst & Young Zurich, where I finished my internship, and Mrs. Van't Dack for their helpful comments and suggestions for the paper.

Finally, my deep thanks go to my family whose support has seen me through the writing of this paper, and especially to my mother and my sister.

Geneva – Zurich - Lugano

2007